

Listing of Claims:

1. (Previously presented) A method of improving security processing in a computing network, comprising:

providing a security offload component in an operating system kernel which performs security processing;

providing control functions in the operating system kernel for directing operation of the security offload component;

providing an application program;

executing the application program; and

executing the provided control functions during execution of the application program, thereby selectably directing the security offload component to secure at least one communication of the executing application program.

2. (Previously presented) The method according to Claim 1, wherein the executing control functions comprises a function directing the security offload component to begin securing the communications.

3. (Previously presented) The method according to Claim 1, wherein the executing control functions comprises a function directing the security offload component to stop securing the communications.

4. (Original) The method according to Claim 2, wherein the function further specifies information to be used by the security offload component.

5. (Previously presented) The method according to Claim 4, wherein the specified information comprises at least one of: authentication information; cipher suites options; and security key input information.

6. (Original) The method according to Claim 1, wherein the control functions further

inform protocol layers of the operating system kernel to modify outbound data in preparation for use by the security offload component.

7. (Previously presented) The method according to Claim 6, wherein the modifications comprise reserving space in the outbound data for security headers and trailers.

8. (Previously presented) The method according to Claim 1, wherein the control functions comprise providing at least one of client and/or server certificates to the security offload component for use in securing the communications.

9. (Previously presented) The method according to Claim 1, wherein the control functions comprise providing at least one key or key ring to the security offload component for use in securing the communications.

10. (Previously presented) The method according to Claim 1, wherein the control functions comprise providing an identification of an encryption algorithm to the security offload component for use in securing the communications.

11. (Original) The method according to Claim 1, wherein secured outbound data of the executing application is thereby sent to its destination directly from the security offload component, after a single pass over a data bus from a protocol stack of the operating system kernel.

12. (Previously presented) A system for improving security processing in a computing network, comprising:

a security offload component in an operating system kernel which performs security processing;

at least one control function in the operating system kernel for directing operation of the security offload component;

means for executing the at least one provided control function; and

means, responsive to operation of the means for executing, for directing the security offload component to secure at least one communication of an application program.

13. (Previously presented) A computer program product for improving security processing in a computing network, the computer program product embodied on at least one computer-readable media and comprising:

a security offload component in an operating system kernel which performs security processing;

at least one control function in the operating system kernel for directing operation of the security offload component;

computer-readable program code for executing the at least one provided control function; and

computer-readable program code, responsive to operation of the computer-readable program code for executing, for directing the security offload component to secure at least one communication of an application program.

14. (Previously presented) The system according to Claim 12, wherein the means for executing comprises means for directing the security offload component to begin securing the communications.

15. (Previously presented) The system according to Claim 12, wherein the means for executing comprises means for directing the security offload component to stop securing the communications.

16. (Previously presented) The system according to Claim 12, wherein the at least one control function further informs protocol layers of the operating system kernel to modify outbound data in preparation for use by the security offload component.

17. (Previously presented) The system according to Claim 12, wherein secured outbound data of the application program is thereby sent to its destination directly from the

security offload component, after a single pass over a data bus from a protocol stack of the operating system kernel.

18. (Previously presented) The computer program product according to Claim 13, wherein the computer readable program code for executing comprises computer readable program code for directing the security offload component to begin securing the communications.

19. (Previously presented) The computer program product according to Claim 13, wherein the computer readable program code for executing comprises computer readable program code for directing the security offload component to stop securing the communications.

20. (Previously presented) The computer program product according to Claim 13, wherein the at least one control function further informs protocol layers of the operating system kernel to modify outbound data in preparation for use by the security offload component.